Fig. 1

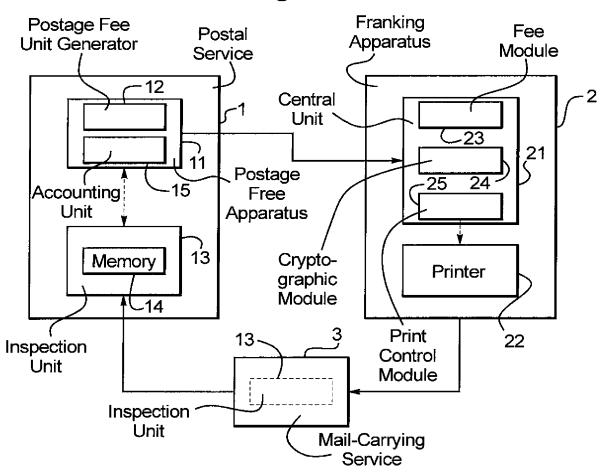
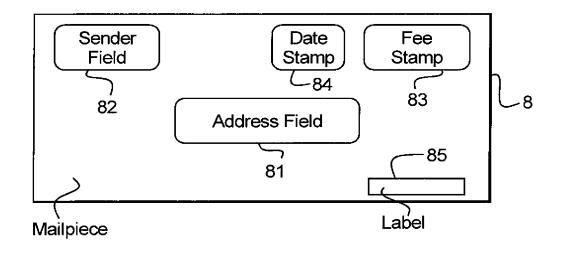


Fig. 2



SCHIFF HARDIN LLP Inventor(s): <u>Gerrit Bleumer</u> Sheet <u>2</u> of <u>5</u> Case No. <u>P00,1748</u> USSN <u>09/728,741</u> Conf # <u>2355</u> GAU <u>3685</u>

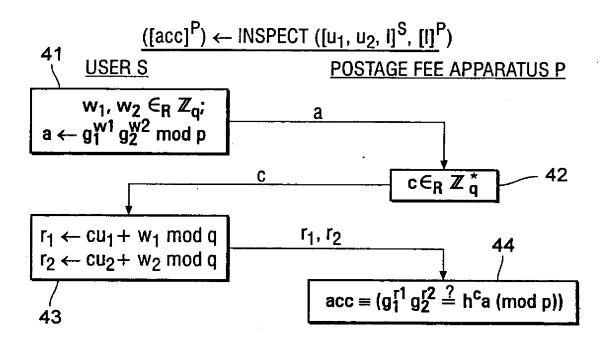


Fig. 3

(s)
$$\leftarrow$$
 indicium (A, B, α , β , (z, a, b, r), rcpt, d/t)

<u>USER S</u>

$$c \leftarrow \mathcal{X}(A, B, z, a, b, r, rcpt, d/t)$$

 $s = (s_1, s_2, s_3), \text{ wherein } s_i \leftarrow \alpha_i + c\beta_i \text{ for } i = 1,2,3$

Fig. 5

(u₁, u₂) IDENTIFY DS (c1,s1,c2,s2)

INSPECTION UNIT

$$\begin{array}{c} u_1 \leftarrow \frac{s_{11} \ (c_2 - 1) + s_{21} \ (1 - c_1)}{s_{13} \ (c_2 - 1) + s_{23} \ (1 - c_1)} \ \text{mod p} \\ u_2 \leftarrow \frac{s_{12} \ (c_2 - 1) + s_{22} \ (1 - c_1)}{s_{13} \ (c_2 - 1) + s_{23} \ (1 - c_1)} \ \text{mod p} \end{array}$$

Fig. 6

SCHIFF HARDIN LLP Inventor(s): <u>Gerrit Bleumer</u> Sheet <u>3</u> of <u>5</u> Case No. <u>P00,1748</u> USSN <u>09/728,741</u> Conf# <u>2355</u> GAU <u>3685</u>

$\underline{([A',B',\alpha,\beta,\sigma']^S)} \leftarrow \text{DOWNLOAD} ([u_1, u_2, y, l], [x, l]^P)$

USER S POSTAGE FEE APPARATUS P $([acc]^P) \leftarrow INSPECT ([u_1, u_2, I]^S, [I]^P)$ CONTINUE IF acc 53 SELECT t∈RZq X $u \in_R \mathbb{Z}_q^*, v \in_R \mathbb{Z}_q$ z, a, b $z \leftarrow (IG_0)^3$ $(a, b) \leftarrow (G^t, (IG_0)^t)$ $\mathbf{w} \in_{\mathbf{R}} \mathbb{Z}_{\mathbf{q}}, \alpha \in_{\mathbf{R}} \mathbb{Z}_{\mathbf{q}}^3$ SELECT $(l', z') \leftarrow ((lG_0)^{\hat{W}}, z^{\hat{W}})$ $A' \leftarrow g_1^{\alpha 1} g_2^{\alpha 2} G_0^{\alpha 3}$ $\beta \leftarrow (u_1 w - \alpha_1, u_2 w - \alpha_2, w - \alpha_3)$ $\mathbf{B}' \leftarrow \mathbf{g}^{\beta 1} \mathbf{g}^{\beta 2} \mathbf{g}^{\beta 3}$ 54 { as of now : $A'B' = I' \mod p$ } $(a', b') \leftarrow (a^U g^V, b^{WU} I^V)$ $c' \leftarrow \mathcal{R}(A', B', z', a', b')$ $c \leftarrow \frac{C'}{C'} \mod q$ $r \leftarrow cx + t$ $r' \leftarrow ru + v$

CONTINUE IF VERIFY

Po P (y, A', B', (z', a',b', r'))

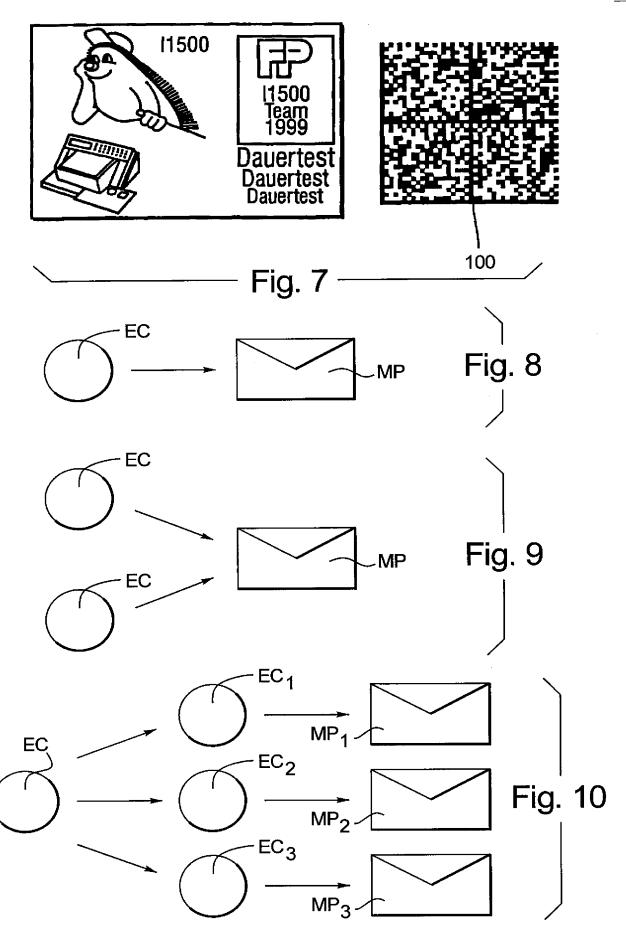
 $\sigma' \leftarrow (z', a', b', r')$

Fig. 4

56

SCHIFF HARDIN LLP

Inventor(s): <u>Gerrit Bleumer</u>
Sheet 4 of 5 Case No. <u>P00.1748</u>
USSN <u>09/728,741</u> Conf # <u>2355</u> GAU <u>3685</u>



SCHIFF HARDIN LLP Inventor(s): Gerrit Bleumer Sheet _5 _ of _5 _ Case No. <u>P00,1748</u> USSN <u>09/728,741</u> Conf # <u>2355</u> GAU <u>3685</u>

